Attorney Docket: 2002_0211A

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICANT: Kenji IWANO et al.

SERIAL NO.:   10/067,843   GROUP:

FILED: February 8, 2002   EXAMINER:

FOR: MEDICAL INFORMATION SYSTEM

VERIFICATION OF ENGLISH TRANSLATION

Honorable Commissioner of Patents
and Trademarks
Washington, D.C. 20231

Dear Sir:

    I, the below named translator, hereby declare that:

    My name and post office address are as stated below:

    That I am knowledgeable in the English language and in the Japanese language in which the above-identified application was filed at the USPTO on February 8, 2002 under Serial No. 10/067,843, and that I believe the attached English translation is a true and complete translation of said U.S. application.

    I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.
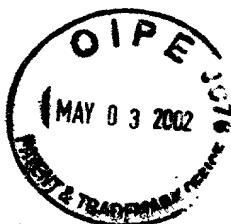
Date: March 27, 2002
Name: Yoshiyuki MAEHORI

Signature: _Yoshiyuki Maehori_
Address: c/o AOYAMA & PARTNERS,
IMP Building 16F, 1-3-7, Shiromi,
Chuo-ku, Osaka 540-0001 Japan

MEDICAL INFORMATION SYSTEM

BACKGROUND OF THE INVENTION

[0001]   The present invention relates to a medical information system adapted to a home health care.

[0002]   Recently, medical information systems have been provided. In the medical information systems, vital information of home care patients is collected through a network, and the vital information collected through the network can be browsed.   For instance, a system disclosed in Japanese laid-open patent publication No. 8-38435 has a plurality of patient terminals for transmitting measured vital data, a single of server for storing and managing the vital data received from these patient terminals, and a plurality of doctor terminals for obtaining or browsing the vital information retained in the single of server.

[0003]   However this system provided with the single of server has following problems.

[0004]   First, load to the server at data correction processes is increased with increasing of the number of the patient terminals.   The loads to the server at data browsing processes are also increased with the increasing of the number of the patient terminals.   These increases of the loads to the server cause a delay in response time and decreasing in a transmission rate. Especially, extremely heavy loads to the server may result in that the data collection from the patient terminals and the data browsing from the doctor terminals would be impossible.

[0005]   Second, while the sever is downed to modify a program installed

therein so as to adapt the program to changes in specification or addition of the patient terminal, the data browsing from the doctor terminals is impossible. Similarly, in case of changes in specification or addition of the doctor terminal, the data collection from the patient terminals is impossible due to the down of the server for changing the program.

[0006] Third, the single server can not satisfy both requirements from a system administrator and requirements inconsistent with the system administrator's requirement from medical institutions such as hospitals that are users of the doctor terminals. Specifically, the system administrator generally demands to hold the server so as to operate and manage it. Contrarily to this, the medical institutes demand to hold the server so as to make it able to use the vital data collected from the patient terminals in other medical information systems such as an electronic chart system.

[0007] Fourth, the single server has a low level of security property. Specifically, third parties with bad faith may access to the vital information by using the patient terminal without proper authentication.

SUMMARY OF THE INVENTION

[0008] With consideration to problems regarding above-mentioned conventional medical information systems, objects of the present invention are to reduce the loads to the server, enhance flexibility of the system, and improve security properties.

[0009] Therefore, a first aspect of the present invention provides a medical information system comprising: a patient server that can receive

vital information, firstly retain the received vital information, and transmit the retained vital information; and a medical care provider server connected to the patient server through a first network, the medical care provider server being capable of retaining the vital information received from the patient server through the first network and allowing the retained vital information to be browsed or viewed.

[0010]   The medical information system further comprises a patient terminal connected to the patient server through a second network, the patient terminal being capable of transmitting the vital information to the patient server through the second network; and a doctor terminal connected to the medical care provider server through a third network, the doctor terminal being capable of browsing the vital information retained in the medical care provider server through the third network.

[0011]   In the medical information system according to the first aspect of the invention, the patient server processes collection of the vital information from the patient terminal, whereas medical care provider server processes browsing of the vital information by the doctor terminal. In other words, in the medical information system, the processes are decentralized by concurrent processes in the servers, thereby reducing loads to each of the respect servers.   Thus, response time is shortened, resulting in improvement of communication speed. Further, stability of the system is improved by reducing the loads to the patient server and the medical care provider server. This enables the collection of the vital information form the patient terminal and the browsing of the vital information by the doctor terminal to be always executed in a stable manner.

[0012]   The patient terminal is connected to the patient server, whereas the doctor terminal is connected to the medical care provider server. Accordingly, when a server program is modified so as to adapt the program to changes in specification or addition of the patient terminal, only the patient server needs to be downed, whereas the browsing of the vital information retained in the medical care provider server by the doctor terminal can be continued.   Controversy, when the server program is modified so as to adapt the program to changes in specification or addition of the doctor terminal, only the medical care provider server needs to be downed, whereas the collection of the vital information by the patient server can be continued.

[0013]   The system administrator can hold the patient server to operate and manage it, thereby the maintenance and operation of the data being simplified.   On the other hand, the medical institute can hold the medical care provider server so as to use the vital information retained in the medical care provider server for other medical information systems such as the electronic chart system.   In these meanings, the medical information system according to the first aspect of the present invention has high flexibility.

[0014]   Specifically, the patient terminal is provided with a sensor for measuring vital data, and the vital information includes a measured value by the sensor.

[0015]   The medical care provider server can transmit the inquiry received from the doctor terminal to the patient server through the first network.   The patient server may transmit the inquiry received from the

medical care provider server to the patient terminal through the second network. The vital information transmitted from the patient terminal to the patient server through the second network may include a reply to the inquiry transmitted to the patient terminal.

[0016]   Preferably, the medical information system includes a first unauthorized access prevention section provided in the first network, a second unauthorized access prevention section provided in the second network and a third unauthorized access prevention section provided in the third network. The first and third unauthorized access prevention sections preferably have higher security levels than that of the second unauthorized access prevention section.

[0017]   For instance, the first unauthorized access prevention section is provided with a firewall and a virtual private network, the second unauthorized access prevention section is provided with a remote access server, and the third unauthorized access prevention section is provided with a terminal authentication server.

[0018]   The patient server only can be accessed directly from the patient terminal through the second network. Further, the first unauthorized access prevention section provided in the first network for communicating the patient server and the medical care provider server has higher security level than that of the second unauthorized access prevention section. Accordingly, unauthorized access from the patient server to the vital information retained in the medical care provider server can be prevented. Also, The lower security level of the second unauthorized access prevention section than those of the first and third unauthorized access prevention

sections ensures a convenient connection from the patient terminal to the patient server. The high security level of the third network for connecting the doctor terminal and the care provider server prevents unauthorized access in direct to the medical care server. In these meanings, the medical information system according to the first aspect of the present invention has very high level of security.

[0019] The patient server and the medical care provider server may be respectively clustered. Clustering of the patient server and the medical care provider server makes it possible to realize further decentralization of the loads to them. The clustering also improves fault tolerance and makes it possible to realize a system that does not stop 24 hours a day.

[0020] A second aspect of the invention provides a medical information system comprising: a plurality of patient servers that can receive vital information, firstly retain the received vital information, and transmit the retained vital information; a medical care provider server connected to the patient servers through a first network, the medical care provider server being capable of retaining the vital information received from the patient servers through the first network and allowing the retained vital information to be browsed; a plurality of patient terminals respectively connected to the patient server through a second network, the patient terminals being capable of transmitting the vital information to the patient server through the second network; and a doctor terminal connected to the medical care provider server through a third network, the doctor terminal being capable of browsing the vital information retained in the medical care provider server through the third network.

[0021]   In the medical information system according to the second aspect of the present invention, when a server program is modified so as to adapt the program to change in specification or addition of the patient terminals connected to one of the plurality of patient servers, only corresponding patient server needs to be downed.   The other patient servers can continue to collect the vital information form the patient terminals connected thereto.

[0022]   A third aspect of the present invention provides a medical information system comprising: a patient server that can receive vital information, firstly retain the received vital information, and transmit the retained vital information; a plurality of medical care provider servers respectively connected to the patient server through a first network, the medical care provider servers being capable of retaining the vital information received from the patient server through the first network and allowing the retained vital information to be browsed; a patient terminal connected to the patient server through a second network, the patient terminal being capable of transmitting the vital information to the patient server through the second network; and a plurality of doctor terminals respectively connected to the medical care provider server through a third network, the doctor terminals being capable of browsing the vital information retained in the medical care provider servers through the third network.

[0023]   In the medical information system according to the third aspect of the present invention, the plurality of medical care provider servers can be respectively held and managed by corresponding medical institutes. Accordingly, each of the medical institutes can retain the vital information

in its medical care provider server for long term. Further, views at doctor terminals when the vital information is browsed can be customized in accordance with each of the medical institutes.

BRIEF DESCRIPTION OF THE DRAWINGS

[0024]   Further objects and advantages of the present invention will become clear from the following description taking in conjunction with the preferred embodiments thereof with reference to the accompanying drawings, in which:

[0025]   Fig. 1 is a block diagram showing a medial information system according to a first embodiment of the present invention;

[0026]   Fig. 2 is a schematic block diagram showing the medical information system according to the first embodiment of the present invention;

[0027]   Fig. 3 is a flow chart for explaining measurement of vital information;

[0028]   Figs 4A and 4B are respectively a flow chart for explaining transmission of the vital information from a patient terminal to a patient server;

[0029]   Figs. 5A and 5B are respectively a flow chart for explaining transmission of the vital information from the patient server to a medical care provider server;

[0030]   Figs. 6A and 6B are respectively a flow chart for explaining browsing of the vital data retained in the medical care provider server by a doctor terminal;

[0031]   Figs. 7A and 7B are respectively a flow chart for explaining transmission of a medical inquiry from the doctor terminal to the medical care provider server;

[0032]   Figs. 8A and 8B are respectively a flow chart for explaining transmission of the medical inquiry from the care provider to the patient server;

[0033]   Figs. 9A and 9B are respectively a flow chart for explaining transmission of a reply to the medical inquiry from the patient server to the patient terminal;

[0034]   Fig. 10 is a schematic view showing an example of a data structure of the patient server;

[0035]   Fig. 11 is a schematic view showing an example of a data structure of the medical care provider server;

[0036]   Fig. 12 is a schematic block diagram showing a medical information system according to a second embodiment of the present invention;

[0037]   Fig. 13 is a schematic block diagram showing a medical information system according to a third embodiment of the present invention;

[0038]   Fig. 14 is a schematic block diagram showing a medical information system according to a fourth embodiment of the present invention; and

[0039]   Fig. 15 is a schematic block diagram showing an example of a clustered patient server.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

First Embodiment

[0040]   As illustrated in Figs. 1 and 2, a medical information system according to a first embodiment of the present invention is provided with a patient server (PS) 1 and a medical care provider server (CPS) 2 connected with each other through a first network 3A.   Further, this medical information system is provided with a plurality of patient terminals (PT) 4 respectively connected to the patient server 1 through a second network 3B, and a plurality of doctor terminals (DT) 5 connected to the medical care provider server 2 through a third net work 3C.

[0041]   In outline, vital data is transmitted from the patient terminal 4 to the patient server 1 through the second network 4.   As described later, the vital data includes a measurement value and a reply to a medical inquiry (inquiry).   The patient server 1 temporally retains the vital data received from the patient terminals 4.   The patient server 1 transmits the vital data retained therein to the medical care provider server 2 through the first network 3A in accordance with a request from the medical care provider server 2.   The medical care provider server 2 retains the vital information received from the patient serer 1.   The data stored in the medical care provider server 2 can be browsed or viewed from the doctor terminal through the third network 3C.

[0042]   The patient terminal 4, for instance, consists of a personal computer to which a plurality of sensors 7 for measuring the vital data of patients are connected.   Such kind of sensors for example, includes a hemadynamometer and a scale.

[0043] Software construction of the patient server 1 will be described. First, the patient server 1 is provided with Web server software 10b which runs on an operating system 10a. For example, Windows 2000® from Microsoft may be adopted as the operating system 10a. Further, Internet Information Server® (IIS), for example, may be adopted as the Web server software 10b. Furthermore, operated on an application execution environment 10c are application server software 10d, a server program 10e, and a database driver 10f. Java Virtual Machine® (JVM) from Javasoft, for example, can be adopted as the application execution environment 10c. Further, JRUN® from Macromedia can be adopted as the application server software 10d. Furthermore, JDBC® from Inet can be adopted as the database driver 10f. According to commands form the server program 10e, the database driver 10f manipulates database files 10h using a database server 10g as an interface.

[0044] Similarly to the patient server 1, the care provider server 2 is provided with web server software 11b (e.g. IIS from Microsoft) operated on an operating system 11a (e.g. Windows 2000® from Microsoft). Further, operated on an application execution environment 11c (e.g. JVM from Jabasoft) are application server software 11d (e.g. JRUN from Macromedia), a server program 11e, and a database driver 11f (e.g. JDBC from Inet). The database driver 11f manipulates database files 11h using a database server 11g as an interface. Furthermore, the medical care provider server 2 is provided with HTML and a scrip 11i manipulated on the Web server software 11b.

[0045] The doctor terminal 5 consists of, for example, a normal personal

computer. As described later, the doctor terminal 5 is provided with browser software for communicating with the medical care provider server 2.

[0046]   The first network for connecting the patient server 1 and the medical care provider server 2 is provided with a firewall 12A and a virtual private network (VPN) 13A for the patient server 1 as well as a firewall 12B and a VPN 13B for the medical care provider server 2.

[0047]   The second network for communicating each of the patient terminals 4 and the patient server 1 is provided with a remote access server (RAS) 15 connected to each of the patient terminals 4 through a phone line 14 and a local area network 16.

[0048]   The third network 3C for communicating each of the doctor terminals 5 and the medical care provider server 2 is provided with a terminal authentication server 18.

[0049]   Operation of the medical information system will be described below with reference to flow charts in Figs. 3 to 9B.

[0050]   First, measurement of the vital data in the patient terminal 4 will be described with reference to Fig. 3. At step S301, the sensor 7 for measuring performs measurement of the vital data such as blood pressure, body temperature, or body weight. Then, if the patient terminal 4 receives the vital data at step S302, then it retains the data in its memory at step S303.

[0051]   Figs. 4A and 4B illustrate processes until the vital data retained in the memory of the patient terminal 4 is transmitted to the patient server 1. In addition to above-mentioned measurement value such as the blood pressure or body temperature, the vital data retained in the memory of the

patient terminal 4 includes the reply to the inquiry that have been transmitted to the patient server 4 from the doctor terminal 5 through the medical care provider server 2 and the patient server 1. First, at step S401, the patient terminal 4 requires access to the RAS 15 by meahs of dial-up connection through the phone-line 14. The RAS 15 performs authentication of the patient terminal 4 being requiring the access by means of password at step S409, and then transmits a result of the authentication to the patient terminal 4 at step S410. If the authentication has been denied at step S402, then the patient server 4 performs error display at step S403 and disconnects the dial-up connection at step S408. On the other hand, if the authentication has been approved at step S402, the patient terminal 4 checks whether or not there is a vital data not transmitted yet in the memory. If the any vital data not transmitted yet exits, then the patient terminal 4 transmits a request for data transmission to the patient server 4 at step S405. After receiving the request at step S411, in case that activation of the server program 10e succeeds at step S412, the patient server 1 performs connection to the database files 10h at step S413. Further, in case that the connection to the database files 10h has been succeeded at step S414, the patient server 1 writes the data to the database files 10h at step s415 followed by disconnection of the database files 10h at step S416. On the other hand, in case that the activation of the server program 10e has failed at step S412, an error message is generated at step S418. Lastly, the patient server 1 transmits a response to the patient terminal 4 at step S417.

[0052] After receiving the response from the patient server 1 at step

S406 and updating a screen view at step S407, the patient terminal 4 disconnects the dial-up connection at step S408.

[0053]   Figs. 5A and 5B illustrate processes until the vital data has been transmitted from the patient server to the medical care provider server 2.

[0054]   First, subsequent to transmission of a connection request from the patient server 1 to the medical care server 2 at step S501, the firewall 12B for the medical care provider server 2 performs authentication at step S502.   If the authentication by the firewall 12B has been approved at step S503, then the VPN 13B for the medical care provider server 2 performs further authentication at step S504.   In case that the authentication by the VPN 13B has been approved at step S505, that connection to the medical care provider server 4 is possible at step S506, and that the patient server 1 can be connected to the database files 10h thereof at step S507, the patient server 1 requests the medical care provider server 2 to connect to the database files 11h.   On the other hand, in case that the connection to the medical care provider server 2 is impossible at step S506, or that the connection to the database files 11h is impossible at step S507, the patient server 1 performs the error display at step S515.

[0055]   If the connection to the database files 11h is possible at step S517, then the medical care provider server 2 informs an existence of the possibility to the patient server 1.   On the other hand, if the connection to the database files 11h is impossible at step S 517, the medical care provider server 2 performs error display.

[0056]   If the patient server 1 has received the possibility for connection to the database files 11h from the medical care provider server 2 at step

S509, the patient server transmits the vital data to the medical care provider server 2 at step S510. The transmitted vital data is received by the medical care provider server 2 at step S518 ,and then retained in the database files 11h. Next, the medical care provider server 2 transmits a transfer result to the patient server 1 at step S519 and disconnects the connection to the database files 11h at step S520.

[0057]   After receiving the transfer result from the medical care provider server 2 at step S511, the patient server disconnects the connection to the database files 10h at step S512 and stores the transfer result in the memory. Then, the patient server 1 disconnects connection to the VPN 13B.

[0058]   Browsing of the vital information stored in the medical care provider server by the doctor terminal 5 will be described below with reference to Figs. 6A and 6B.

[0059]   The doctor terminal 5 activates browser software installed therein at step S601 and accesses to a home page set up in the medical care provider server 2. The terminal authentication server 18 performs authentication of the doctor terminal 5 seeking the access at step S616 and transmits a result of the authentication to the doctor terminal 5 at step S617. It should be noted that the doctor terminal has obtained certification issued by the terminal authentication terminal 18 in advance. Specifically, provided that the data regarding particular doctor terminal is registered to a institution managing the medical information system such as a management center, the certification is (electronically) issued by the terminal authentication server 18 to the doctor terminal 5. Using identification data included in the certification and registered in the doctor

terminal 5, the terminal authentication server 18 performs the authentication when the doctor terminal 5 tries to access to the home page. Alternatively, using the certification (electronically) issued by the terminal authentication server 18 and introduced to the doctor terminal 5 through a medium that is not duplicable (e.g. floppy disk, IC card, or onetime password generator), the terminal authentication server 18 performs the authentication when the doctor terminal tries to access.

[0060] In case that the authentication has been approved at step S606 and that the connection to the medial care provider server is possible at step S604, a login screen is displayed at step S605. Then, the medical care provider server 2 performs authentication of the doctor terminal 5 requiring the login at step S619 and transmits a result of the authentication to the doctor terminal 5 at step S620. If the authentication has been approved at step S606, the doctor terminal logs in to the server. Further, the doctor terminal 5 transmits to the medical care provider server 2 a request for selecting a patient whose information is sought to be browsed at step S608 and a request for selecting vital data required to be browsed at step S609. Then, the doctor terminal 5 transmits a request for browsing vital data to the medical care provider server 2 at step S610.

[0061] The medical care provider server 2 receives these requests at step S622. If activation of the server program 11e is succeeded at step S624, then the care medical care provider server 2 performs connection to the database files 11h. If the connection to the database files 11h has been succeeded at the step S625, the medical care provider server 2 obtains the vital data corresponding to the requests from the doctor terminal 5 (steps

S608 and S609) and then disconnects the connection to the database files
11h. On the other hand, in case that the activation of the server program
11e has not succeeded at step S623 or that the connection to the database
files 11h is impossible at step S625, an error message is generated at step
S631.

[0062] Further, the medical care provider server 2 creates a response to
the doctor terminal 5 in HTML format at step S628 and transmits the
response to the doctor terminal 5 at step S629. The response includes the
requested vital information or the error message. Unless the doctor
terminal 5 loges out at step S630, the medical care provider server continues
to perform processes after step S622.

[0063] Next, transmission of the inquiry from the doctor terminal 5 to
the medical care provider server 2 will be described with reference to Figs.
7A and 7B. First, the doctor terminal 5 activates browser software
installed therein at step S701 and accesses to the home page for the doctor
terminals at step S702. The terminal authentication server 18 performs
authentication of the doctor terminal 5 seeking the access at step 716, and
then transmits a result of the authentication to the doctor terminal at step
S717. In case that the authentication has been approved at step S703 and
that the connection to the medical care provider server 2 is possible at step
S704, the login screen is displayed at step S705. Then, the medical care
provider server 2 performs authentication of the doctor terminal 5 requiring
the login at step S718 and transmits a result of the authentication to the
doctor terminal 5 at step S620. It should be noted that the doctor terminal
5 has obtained certification issued by the terminal authentication server 18

in advance as well as the doctor terminal 5 at browsing of the vital data. If the authentication has been approved at step S706, the doctor terminal 5 logs in to the server at step S707. Further, selection of a patient to whom the inquiry is to be sent is performed at step S708, and then setting of contents of the medical inquiry is performed at step S709. The contents of medical inquiry include items such as whether or not taking meals or sleeping time. However, the contents of the inquiry are not limited. The doctor who is the user of the doctor terminal 5 can set the contents depending on particular user who is the user of the patient terminal 1 and his or her medical condition. Then, a request for transmitting the medical inquiry is transmitted from the doctor terminal 5 to the medical care provider server 2 at step S710.

[0064] The medical care provider server 2 receives the request for transmitting the medical inquiry at step S721 and if activation of the server program 11e is succeeded at step S722, then the medical care provider server 2 performs connection to the database files 11h at step S723. If the connection to the database files 11h has been succeeded at step S724, then the medical care provider server 2 stores the data of the medical inquiry transmitted from the doctor terminal 5 in the database files 11h, followed by disconnecting the connection to the database files 11h at step S726. On the other hand, in case that the activation of the server program 11e has not succeeded at step S722 or that the connection to the database files 11h are impossible at step S625, an error message is generated at step S730.

[0065] Further, the medical care provider server 2 creates a response to the doctor terminal 5 in HTML format at step S727 and transmits the

response to the doctor terminal 5 at step S728. The response includes the contents of the inquiry received from the doctor terminal 5 or the error message. After the doctor terminal 5 receives the response at step S711, the inquiry is displayed at step S712. If another inquiry is to be set at step S713, then the processes after step S709 are repeated. If another patient is to be selected at step S714, then the processes after step S708 are repeated. Unless the doctor terminal 5 has logged out at step S729, the processes after step S721 are repeated.

[0066] Figs. 8A and 8B illustrate processes until the inquiry is transmitted from the medical care provider server 2 to the patient server 1. Subsequent to transmission of a connection request from the medical care provider server 2 to the patient server 1 at step S801, the firewall 12A for the patient server 1 performs authentication at step S802. If the authentication by the firewall 12A has been approved at step S803, then the VPN 13A for the patient server 1 performs further authentication at step S804. In case that the authentication by the VPN 13A has been approved at step S805, that connection to the patient server 1 is possible at step S806, and that the medical care provider server 4 can connect to the database files 11h thereof at step S807, the medical care provider server 4 requests the patient server 1 to connect to the database files 10h at step S808. On the other hand, in case that the connection to the patient server 1 is impossible at step S806 or that the connection to the database files 11h is impossible at step S807, the medical care provider server 2 performs the error display at step S815.

[0067] If the patient server 1 has been connected to the database files

10h at steps S817 and S809, then the medical care provider server 2 transmits the inquiry to the patient server 1 at step S810. The patient server 1 receives the inquiry and then stores the inquiry in the database files 10h at step S818. Further, after transmitting a transform result to the medical care provider server 2 at step S819, the patient server 1 disconnects the connection to the database files 10h. On the other hand, if the connection to the database files 10h is denied at step S817, then the patient server performs error display at step S821.

[0068] After receiving the transfer result from the patient server 1 at step S811, the medical care provider server 2 disconnects the connection to the database files 11h at step S812. Then, the medical care provider server 2 retains the transfer result in the memory at step S813 and disconnects the connection to the VPN 13A at step S814.

[0069] Next, transmission of the inquiry from the patient server 1 to the patient terminal will be described with reference to Figs. 9A and 9B.

[0070] First, at step S901, the patient terminal 4 requires access to the RAS 15 by means of dial-up connection through the phone line. The RAS 15 performs authentication of the patient terminal 4 being requiring the access by means of password at step S909, and transmits a result of the authentication to the patient terminal 4 at step S910. If the authentication has been denied at step S902, then the patient server 4 performs error display at step S903 and disconnects the dial-up connection at step S908. On the other hand, the authentication has been approved at step S902, then the patient terminal 4 transmits a request for transmission of the medical inquiry to the patient server 1 at step S904. After receiving the request at

step S911, in case that activation of the server program 10e is succeeded at step S912, the patient server 1 performs connection to the database files 10h at step S913. Further, in case that connection to the database files 10h has been succeeded at step S914, the patient server 1 checks whether or not there are any data not transmitted yet at step S915.

[0071]   In case that the inquiry not transmitted to the patient terminal 4 exists, the patient server 1 creates a response for setting the inquiry and then disconnects the connection to the database files 10h. On the other hand, in case that the server program 10h has not been activated at step S912 or that the connection to the database files 10h is impossible at step S914, the patient server 4 creates an error message.

[0072]   The patient terminal 4 receives the response to retain in the memory at step S906. After updating the screen display at step S907, the patient terminal 4 disconnects the dial-up connection at step S908.

[0073]   Fig. 10 illustrates an example of structures of the data stored in the database files 10h. Although body weights of patients and whether or not they take meal are shown in this example, the vital data and the medical inquiry are not limited to these items. As shown in Fig. 10, the patient server 1 stores the vital data for each of IDs respectively allocated to particular patient who is a user of the patient terminal 4. Further, transmission flags in Fig. 10 include information relating to whether or not transfer of the measurement data and the reply to the medical inquiry has been finished. Specifically, a value of "0" for the transmission flag indicates that corresponding data, which is the vital data or the reply to the medical inquiry, has not been finished yet, whereas a value of "1" for it

indicates that the transfer has been already finished.   Concretely, when the

transmission of one measurement value (body weight), e.g. "65.75", is

finished at step S511 in Fig. 6, a transmission flag corresponding to the

measurement value (body weight) is changed from "0" to "1".   This control

of the transmission flag allow the system administrator of the patient server

1 to delete measurement data and the replies having the transmission flag

of "1" in the data retained in the patient server 1, resulting in that the

maintenance of the database is simplified.

[0074]   On the other hand, Fig. 11 illustrates an example of structures of

the data stored in database files 11h of the medical care provider server 2.

Similarly with the data structure of the patient serer 1, the vital data is

stored for each of the IDs allocated respectively to particular patient.

Patient data is also stored for each of IDs.   The patient data includes

information for identifying particular patient such as name.   It should be

noted that the transmission flag in Fig. 11 has same function as that of the

transmission flag in Fig. 10.

[0075]   As described above, although the patient server 1 stores the vital

data for each of the IDs, it does not store the patient data corresponding to

each of the IDs.   Accordingly, if the patient serer 1 were accessed without

authorization, it would not be impossible to identify each of the vital data

with particular patient.

[0076]   In the medical information system according to the first

embodiment of the invention, the patient server 1 processes collecting of the

vital information from the patient terminals 4, whereas medical care

provider server 2 processes browsing of the vital information by the doctor

terminals 5. In other words, in the medical information system, the processes are decentralized by concurrent processes in the patient server 1 and medical care provider server 2, thereby reducing loads to the respect servers. Thus, response time is reduced, resulting in improvement of communication speed. Further, stability of the system is improved by reducing the loads to the patient server 2 and the medical care provider server 3. This enables the collection of the vital information from the patient terminal 4 and the browsing of the vital information by the doctor terminal 5 to be always executed in a stable manner.

[0077] The patient terminal 4 is connected to the patient server 1, whereas the doctor terminal 5 is connected to the medical care provider server 2. Accordingly, when a server program is modified so as to adapt the program to changes in specification or addition of the patient terminal 4, only the patient server 1 needs to be downed, whereas the browsing of the vital information retained in the medical care provider server 2 by the doctor terminal 5 can be continued. Controversy, when the server program is modified so as to adapt the program to changes in specification or addition of the doctor terminal 5, only the medical care provider server 2 needs to be downed, whereas the collection of the vital information by the patient server 1 can be continued.

[0078] Operation and management of the patient server 1 by the system administrator holding it simplify the maintenance and operation of the data. On the other hand, the medical institute holds the medical care provider server 2 can use the vital information retained in the medical care provider server for other medical information systems such as the electronic chart

system. In these meanings, the medical information system according to the first embodiment has high flexibility.

[0079] The patient server 1 only can be accessed directly from the patient terminal 4 through the second network 3B. Further, the combination of the firewalls 12A, 12B and VPNs 13A, 13B provided in the first network has higher security level than that of the RAS 15 provided in the second network 3B. Accordingly, unauthorized access from the patient terminal 4 to the vital information retained in the medical care provider server 2 can be prevented. Also, the lower security level of the RAS 15 provided in the second network 3B than those of the combination of the firewalls 12A, 12B and the VPNs 13A, 13B provided in the second network 3B and the terminal authentication server 18 provided in the third network 3C ensures a convenient connection from the patient terminal 4 to the patient server 1. The high security level of the third network 3C connecting the doctor terminal 4 and the medical care provider server 2 prevents unauthorized access in direct to the medical care provider server 2. In these meanings, the medical information system according to the first embodiment has very high level of security.

Second embodiment

[0080] Fig. 12 is a schematic view showing a second embodiment of the present invention.

[0081] In this second embodiment, a plurality of patient servers 1A, 1B, ... ,1Z are provided. Further, each of the patient servers 1A, 1B, ... , 1Z is connected to the medical care provider server 2 through the first network 3A. Furthermore, to each of the patient servers 1A, 1B, ... , 1Z, a plurality

of patient terminals 4 are connected. Due to provision of the plurality of patient servers 1A, 1B, ... , 1Z, when a server program is modified so as to adapt the program to change in specification or addition of the patient terminals connected to one of the patient servers 1A, 1B, ... , 1Z, only corresponding patient server needs to be downed. The other patient servers can continue to collect the vital information from the patient terminals connected thereto.

[0082]   Further, in the system according to the second embodiment, where different type of patient terminals 4 (concretely, patient terminals using different type of communication protocols for communication with the patient server) is introduced for collection of the measurement data and the reply to the medical inquiry, the new patient terminals and corresponding patient server can be introduced with continuing management of the existing system.

[0083]   Since other constructions and operations of the second embodiment are same as those of the first embodiment, description is eliminated by allocating same reference numerals to the same elements.

Third Embodiment

[0084]   Fig. 13 illustrates a third embodiment of the present invention.

[0085]   In the third embodiment, a plurality of medical care provider servers 2A, 2B, ... , 2Z are provided. Further, the patient server 1 is connected to the medical care provider servers 2A, 2B, ... , 2Z through the first network 3A. Furthermore, a plurality of doctor terminals 5 are connected to each of the medical care provider servers 2A, 2B, ... , 2Z. Each of the medical care provider servers 2A, 2B, ... , 2Z can be held and managed

by corresponding medical institutes. Accordingly, each of the medical institutes can retain the vital information in the medical care provider server for a long time according to their demand. Further, views at doctor terminals 5 when the vital information is browsed can be customized in accordance with each of the medical institutes. As shown in Fig. 14, a plurality of patient servers 1 and a plurality of medical care provider servers 2 may be provided.

[0086] Since other constructions and operations of the second embodiment are same as those of the first embodiment, description is eliminated by allocating same reference numerals to the same elements.

Fourth Embodiment

[0087] As shown in Fig. 15, in a fourth embodiment, the patient server 2 is clustered. Specifically, the patient server 2 consists of a plurality of server 101A, 101B, ... ,101Z provided in parallel, and appears a single of server when accessed by the patient terminal 4 or medical care provider server 2. This kind of construction is refereed to as clustering. This clustering enables the load to each server to be further decentralized. Due to parallel arrangement of the servers, if the serer 101A is downed for example, the system can continue to be operated by remaining servers 101B, ... , 101N. This improves fault tolerance and makes it possible to realize a system that does not stop 24 hours a day.

[0088] It should be noted that while description about the clustering is made with taking the patient server 2 as a example in this embodiment, the clustering can be adopted also to the medical care provider server.

[0089] Although the present invention has been fully described by way of

the examples with reference to the accompanying drawings, it is to be noted here that various changes and modifications will be apparent to those who skilled in the art. Therefore, unless such changes and modifications otherwise depart from the spirit and scope of the present invention, they should be construed as being therein.